

IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF TENNESSEE
NASHVILLE DIVISION

FILED
U.S. DISTRICT COURT
MIDDLE DISTRICT OF TENN.

AUG 07 2024

UNITED STATES OF AMERICA

NO.: 3:24-00151

v.

MATTHEW ISAAC KNOOT

8 U.S.C. § 1324(a)
18 U.S.C. § 2
18 U.S.C. § 371
18 U.S.C. § 981(a)(1)(A), (C)
18 U.S.C. § 982(a)(1), (2)(B)
18 U.S.C. § 1028A(a)(1)
18 U.S.C. § 1030(a)(5)(A)
18 U.S.C. § 1030(i)
18 U.S.C. § 1349
18 U.S.C. § 1956(h)
21 U.S.C. § 853(p)
28 U.S.C. § 2461(c)


DEPUTY CLERK

INDICTMENT

THE GRAND JURY CHARGES:

INTRODUCTION

1. Since 2003, the Democratic People's Republic of Korea ("DPRK" or "North Korea") has been under sanction by the United Nations ("UN") due to its testing and expansion of its nuclear weapons program. Since 2016, the United States has had comprehensive sanctions against North Korea, cutting it off from the U.S. financial system and limiting the ability of U.S. persons and companies to do business with North Koreans. As a result, North Korea has sponsored various subterfuge schemes to earn money for the regime.

2. According to a May 2022 advisory by the Department of State, the Department of the Treasury, and the Federal Bureau of Investigation, North Korea dispatched thousands of highly skilled information technology ("IT") workers around the world to generate revenue that contributed to North Korea's weapons programs in violation of U.S. and U.N. sanctions. These

North Korean IT workers posed as non-North Korean foreign and U.S.-based remote workers and surreptitiously obtained contracts for remote IT work from companies around the world, including in the United States. According to a March 2024 United Nations Security Council Panel of Experts Report, DPRK IT workers are allowed to keep only a small percentage of their earnings, with the remainder taken by the DPRK government agency that dispatched them. It is estimated that there are thousands of IT workers sent overseas from the DPRK. Additionally, approximately 1,000 DPRK IT workers operate from cities inside North Korea, including from Shinuiju, a city on the border with China.

3. North Korean IT workers commonly obtained these remote IT work contracts through online platforms that allow companies to advertise contracts for IT projects on which freelance IT workers could bid. North Korean IT workers provided prospective employers with counterfeit, altered, or falsified documents, including identification documents, to hide their true identities. To obtain these documents, North Korean IT workers paid individuals and websites for document forgery services or altered authentic identity documents by combining a photo of the North Korean IT worker with the personally identifiable information (“PII”) of another person, including U.S. persons.

4. North Korean IT workers further obfuscated their identities, locations, and nationality by using virtual private networks (“VPNs”) and virtual private servers (“VPSs”). North Korean IT workers also used remote desktop software to access U.S.-based computers so that it appears they are performing their work from U.S.-based locations.

5. North Korean IT workers were aided by both U.S. and foreign facilitators. These facilitators provided a range of services for North Korean IT workers. In particular, U.S. facilitators received and hosted laptops issued by employers to North Korean IT workers and installed remote desktop applications on those laptops, all of which was done in exchange for a fee. These fees

were typically paid to facilitators through online money transfer and digital payment services. North Korean actors favored online payment platforms that provided for cross-border business-to-business payments, cross-border wire transfers, online payments, and refillable debit card services.

6. From in or about July 2022 and continuing through in or about August 2023, the defendant, **MATTHEW ISAAC KNOOT** (“**KNOOT**”), a U.S. citizen and resident of Nashville, Tennessee, acted as a facilitator for one or more overseas IT workers using the persona YANG DI and conspired with them to obtain their employment with U.S. companies, perform work remotely, share in the proceeds generated by the remote IT work, and launder the proceeds of the scheme. This remote IT work was to be performed by individuals physically located within the United States, who were authorized for employment by U.S. companies.

7. JOHN DOE 1, alias YANG DI (“DI”), also known as “Andrew M.,” among other names, was a foreign national residing outside, and not authorized to work in, the United States. DI used the stolen identity of a U.S. citizen (“Andrew M.”) to apply for and obtain remote IT work at U.S. companies.

8. U.S. Victim 1 was a U.S. citizen of Caucasian descent named Andrew M. whose identity was stolen and used to fraudulently obtain remote IT work.

9. **KNOOT** and DI, together with their co-conspirators, are referred to in this Indictment as the “Conspirators.” As part of the conspiracy, **KNOOT** received and hosted laptop computers issued by U.S. companies to Andrew M. at **KNOOT**’s Nashville, Tennessee residences for the purposes of deceiving the companies into believing that Andrew M. was located in the United States. Following receipt of the laptops, and without authorization, **KNOOT** logged on to the laptops, downloaded and installed remote desktop applications, and accessed without authorization the victim companies’ networks. The remote desktop applications enabled DI to work from locations outside the United States, in particular, China, while appearing to the victim

companies that Andrew M. was working from **KNOOT**'s residences. In exchange, **KNOOT** charged DI monthly fees for his services, including flat rates for each hosted laptop and a percentage of DI's salary for IT work, enriching himself off the scheme.

10. As part of their scheme, Conspirators obtained contracts for remote IT work with the following companies:

- a. Company A, whose identity is known to the Grand Jury, was a media company headquartered in New York City, New York.
- b. Company B, whose identity is known to the Grand Jury, was a financial institution headquartered in the United Kingdom with subsidiary corporations located in the United States.
- c. Company C, whose identity is known to the Grand Jury, was a technology company located in Portland, Oregon.
- d. Company D, whose identity is known to the Grand Jury, was a media company located in McLean, Virginia.

11. Conspirators were paid hundreds of thousands of dollars by U.S. companies for remote IT work, which was falsely reported to the Internal Revenue Service ("IRS") and the Social Security Administration ("SSA") in the name of U.S. Victim 1. **KNOOT** was paid \$15,100 for his services, which is substantially less than the \$500 per month, per laptop, plus 20 percent of money earned from the remote IT work that he had agreed to. In addition, the Conspirators caused hundreds of thousands of dollars in damages to the victim companies, which included their costs to investigate the scope of **KNOOT**'s and DI's accesses, audit and otherwise scrutinize the IT projects on which DI worked, and remediate their computers and computer networks following discovery of the scheme.

12. Conspirators then laundered the proceeds of the fraudulent remote IT work scheme using Online Payment Platform 1. Conspirators transferred \$111,893.21 paid by Company A and Company B for remote work purportedly completed by U.S. Victim 1 to four Online Payment Platform 1 accounts registered by individuals claiming to be located in China, whose online accounts utilized the following names: “Jiye Xu,” “tingting sun,” and “chenglong jin.” Two of these accounts—tingting sun and chenglong jin—sent funds to an Online Payment Platform 1 account of a North Korean persona known as “Jiang YuZi.”

COUNT ONE

(Conspiracy to Cause Damage to Protected Computers)

13. The allegations in Paragraphs 1 through 12 of this Indictment are re-alleged here.

14. From in or about July 2022 through at least August 2023, in the Middle District of Tennessee and elsewhere within the jurisdiction of the Court, the defendant, **MATTHEW ISAAC KNOOT**, together with others known and unknown to the Grand Jury, did knowingly conspire and agree to commit the following offenses against the United States:

- a. Knowingly cause the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally caused damage without authorization to protected computers, resulting in loss to one or more persons during a one-year period, and loss and resulting from a related course of conduct affecting one or more other protected computers aggregating at least \$5,000 in value, in violation of Title 18, United States Code, Sections 1030(a)(5)(A), 1030(c)(4)(B), and 1030(c)(4)(A)(i)(I).

Object of the Conspiracy

15. The object of the conspiracy was for **KNOOT**, together with his Conspirators, to generate revenue through a scheme to obtain remote IT work from U.S. companies for overseas

IT workers by downloading and installing software without authorization to enable unauthorized remote access and using stolen U.S. identities, and other means, designed to obscure the true identities and locations of the overseas IT workers.

Manner and Means of the Conspiracy

16. During the course of the conspiracy, and as part of it, the Conspirators used the following manner and means, among others, to achieve its goals:

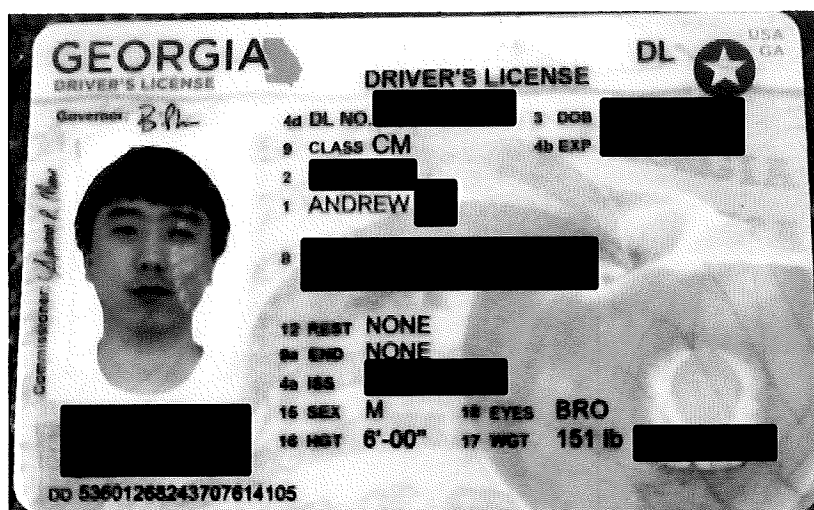
- a. Conspirators purchased, stole, or otherwise obtained PII and other information belonging to at least one U.S. person (U.S. Victim 1), which was used to gain employment with U.S. companies as part of the remote IT work scheme.
- b. Conspirators identified jobs of interest, including jobs with Company A, Company B, Company C, and Company D, in fields such as technology, media, and banking.
- c. Conspirators applied for jobs at the U.S. companies as U.S. Victim 1 and transmitted false information to those companies, DHS, and SSA as part of an employment eligibility check, to include stolen identity information and fake drivers' licenses.
- d. Conspirators directed U.S. companies to ship laptop computers addressed to U.S. Victim 1 to **KNOOT's** residences in Nashville, Tennessee.
- e. Conspirators obtained and shared login credentials to the networks of victim companies, including Company A, Company B, Company C, and Company D to, among other things, perform remote IT work.
- f. Without authorization, Conspirators downloaded software, including but not limited to remote desktop applications, onto laptops belonging to the victim companies, including Company A, Company B, and Company C.

- g. Conspirators transferred money representing payments for the remote IT work between and among accounts provided by U.S. financial institutions and online payment platforms, which were further transferred to overseas actors and to **KNOOT** for his services.

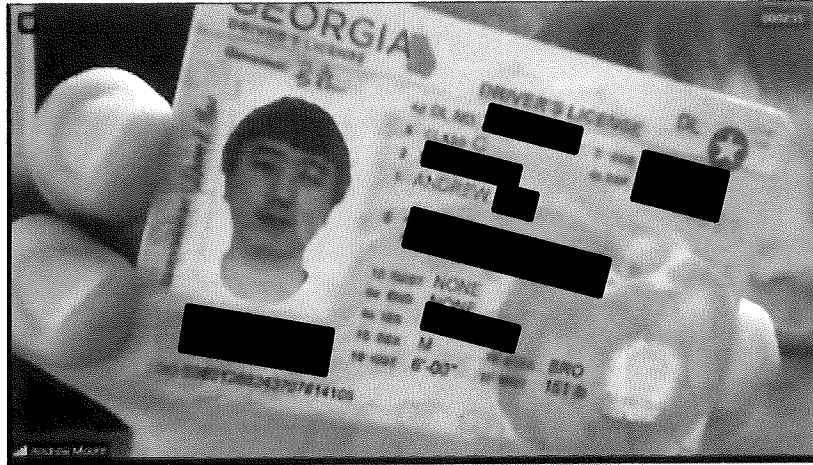
OVERT ACTS

17. In furtherance of this Conspiracy and to accomplish its goals, the following overt acts, among others, were committed in the Middle District of Tennessee and elsewhere:

- a. On or about July 11, 2022, DI, using the name Andrew M. and other means of identification belonging to U.S. Victim 1, obtained employment with Company C, as a senior engineer with a base compensation of \$100,000 per year.
- b. On or about on July 14, 2022, DI, using the name Andrew M. and other means of identification belonging to U.S. Victim 1, obtained employment with Company B, as a mid-level software developer with a base compensation of \$120,000 per year and a bonus of up to 10% of base compensation. During the application process, DI provided a Georgia driver's license containing some of U.S. Victim 1's PII (redacted) as proof of identity:



- c. Between on or about July 21, 2022 and on or about July 22, 2022, **KNOOT** and DI agreed that **KNOOT** would, among other things, receive, set up, and host laptop computers shipped by DI's employers to **KNOOT's** residence, allow DI to use **KNOOT's** online business network account and name, and assist DI with U.S. employment and tax paperwork. DI agreed to pay **KNOOT** \$500 per month per laptop computer and 20 percent of net profits.
- d. On or about July 25, 2022, **KNOOT** received a Windows laptop sent by Company B addressed to Andrew M. at **KNOOT's** residence.
- e. On or about August 3, 2022, DI provided **KNOOT** with login credentials for a Company B laptop, specifically username "Andrew.M[redacted]@[CompanyB].com" and a password, and asked **KNOOT** to configure the laptop for Anydesk or another remote work application. Without authorization, **KNOOT** later used the login credentials provided by DI and installed a remote work application on the Company B laptop.
- f. On or about on August 8, 2022, DI, using the name Andrew M. and other means of identification belonging U.S. Victim 1, obtained employment with Company A, as a developer with a base compensation of \$130,000 per year and a bonus of approximately 7.5% of base compensation. During the application process, which occurred on or about July 21, 2022, DI provided a Georgia driver's license containing U.S. Victim 1's PII (redacted) as proof of identity:



- g. Company A shipped a laptop addressed to Andrew M. at **KNOOT**'s residence. On or about August 8, 2022, DI provided **KNOOT** with login credentials for a Company A laptop, specifically username "andrew.m[redacted]@[CompanyA].com" and a password.
- h. Between on or about August 8, 2022, and on or about August 9, 2022, **KNOOT**, without authorization, connected the Company A laptop to Company A's network and then installed AnyDesk on the Company A laptop.
- i. On or about August 10, 2022, **KNOOT** received a laptop sent by Company C addressed to Andrew M. at **KNOOT**'s residence.
- j. On or about August 9, 2022, **KNOOT** received a laptop sent by Company D addressed to Andrew M. at **KNOOT**'s residence.
- k. On or about August 21, 2022, and without authorization, **KNOOT** used login credentials, specifically username "ANDREW M[redacted]" and a password and, without authorization, installed and ran AnyDesk on the Company C laptop.
- l. From in or about August 2022 through in or about March 2023, Conspirators accessed Company A laptop located at **KNOOT**'s residence from IP addresses

resolving to China in violation of, among other things, Company A's policies relating to both international travel and providing network access to another individual in a high-risk country.

- m. On or about June 22, 2023, **KNOOT** received another laptop, a MacBook Pro, sent by Company B addressed to Andrew M. at **KNOOT**'s residence. Between on or about June 22, 2023 and June 26, 2023, **KNOOT**, without authorization, used login credentials, specifically username "Andrew.M[redacted]@[CompanyB].com and a password and installed and ran Splashtop Streamer on the Company B MacBook Pro.
- n. Beginning on or about July 11, 2022 and ending on or about August 8, 2023, Conspirators caused Company A, Company B, Company C, and Company D to pay the Andrew M. persona—a persona controlled at relevant times by DI—at least approximately \$258,553.74 in wages.
- o. Beginning on or about July 11, 2022 and ending on or about August 8, 2023, Conspirators caused at least \$544,700 in damages to Company A, Company B, and Company C, representing the cost to remediate the victim companies' corporate computer networks and devices, audit code created by DI, and pay associated legal fees.
- p. Beginning on or about July 11, 2022 and ending on or about August 8, 2023, Conspirators paid **KNOOT** approximately \$15,100 for his participation in the scheme.

In violation of Title 18, United States Code, Section 371.

COUNT TWO
(Conspiracy to Commit Money Laundering)

18. The allegations in Paragraphs 1 through 17 of this Indictment are re-alleged here.

19. From in or about July 2022 through at least August 2023, in the Middle District of Tennessee and elsewhere, the defendant, **MATTHEW ISAAC KNOOT**, together with others known and unknown to the Grand Jury, did knowingly conspire and agree to:

- a. knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conduct and attempt to conduct such a financial transaction which in fact involves the proceeds of specified unlawful activity with the intent to promote the carrying on of specified unlawful activity, specifically, computer fraud and wire fraud, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and 1343, in violation of Title 18, United States Code, Section 1956(a)(1)(A)(i); and
- b. knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conduct and attempt to conduct such a financial transaction which in fact involved the proceeds of a specified unlawful activity, that is, computer fraud and wire fraud, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and 1343, knowing that the transaction was designed in whole and in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds of said specified unlawful activity, in violation of Title 18, United States Code, Section 1956(a)(1)(B)(i).

Object of the Conspiracy

20. The object of the conspiracy was for **KNOOT**, together with his Conspirators, to conceal the identity of the remote IT worker and enrich themselves, and each other, by laundering monies earned through fraudulent remote IT work.

Manner and Means of the Conspiracy

21. During the course of the conspiracy, and as part of it, the Conspirators used the following manner and means, among others, to achieve its goals:

a. **KNOOT**, and his Conspirators, conspired to commit computer fraud, as described in Count One of this Indictment, and committed computer fraud, as described in Count Three of this Indictment.

b. **KNOOT**, and his Conspirators conspired to commit wire fraud, as described in Count Three of this Indictment.

c. On or about January 5, 2021, Conspirators using the name “Levani Erkomaishvili,” opened an account at Online Payment Platform 1, a U.S.-based online money transfer and digital payment service (the “Erkomaishvili Account”).

d. On or about January 5, 2021, Conspirators were provided an account at a U.S. financial institution located in Georgia ending in 49277 (the “49277 Account”) in order to receive salary payments fraudulently earned from remote IT work employment obtained using the stolen identity of a U.S. citizen (U.S. Victim 1).

e. Between on or about August 18, 2022, and March 31, 2023, Conspirators caused Company A to transfer \$56,276.98 from its bank account based in the United States to the 49277 Account for work purportedly performed by U.S. Victim 1.

f. Between on or about August 11, 2022, and April 13, 2023, Conspirators caused Company B to transfer \$60,310.04 from its bank account based in the United States to the 49277 Account for work purportedly performed by U.S. Victim 1.

g. Between August 12, 2022, and March 31, 2023, Conspirators transferred the funds paid by Company A and Company B from the 49277 Account to the Erkomaishvili Account.

h. Between September 2, 2022, and March 31, 2023, Conspirators transferred \$111,893.21 from the Erkomaishvili Account to four other Online Payment Platform 1 accounts. Three accounts were registered by individuals claiming to be located in China: Jiye Xu, tingting sun, and chenglong jin. Two of these accounts—tingting sun and chenglong jin—sent funds to an Online Payment Platform 1 account of a North Korean persona known as “Jiang YuZi.” The fourth account was registered by an individual claiming to be located in Bangladesh, named Mst Nasima Khatun.

i. Between August 31, 2022, and July 3, 2023, Conspirators made twelve payments to **KNOOT** through Online Payment Platform 1 account opened in his name, totaling \$15,100, which **KNOOT** transferred to an account in his name at a U.S. financial institution located in Chicago, Illinois, less transactions fees. Six of the payments to **KNOOT** were sent from Online Payment Platform 1 accounts that had received Company A and Company B payments via the Erkomaishvili Account. These payments to **KNOOT** are:

Payment Date	Amount (USD)	Sender Country	Sender First Name	Sender Last Name
1/30/2023	1,100	Bangladesh	MST NASIMA	KHATUN
11/30/2022	1,600	China	tingting	sun
11/2/2022	1,600	China	tingting	sun
9/29/2022	1,600	China	chenglong	jin
8/31/2022	1,900	China	tingting	sun
8/31/2022	100	China	tingting	sun

In violation of Title 18, United States Code, Section 1956(h).

COUNT THREE
(Conspiracy to Commit Wire Fraud)

22. The allegations in Paragraphs 1 through 21 of this Indictment are re-alleged here.

23. From in or about July 2022 through at least August 2023, in the Middle District of Tennessee and elsewhere, the defendant, **MATTHEW ISAAC KNOOT**, together with others

known and unknown to the Grand Jury, did knowingly conspire and agree to commit an offense against the United States, that is, to knowingly devise and intend to devise a scheme and artifice to defraud and for obtaining money and property by means of materially false and fraudulent pretenses, representations, and promises, for which one or more Conspirators transmitted and caused to be transmitted by means of wire communications in interstate and foreign commerce certain writings, signs, signals, pictures, and sounds, for the purpose of executing the scheme and artifice to defraud, in violation of Title 18, United States Code, Section 1343.

In violation of Title 18, United States Code, Section 1349.

COUNT FOUR
(Intentional Damage to a Protected Computer)

24. The allegations in Paragraphs 1 through 23 of this Indictment are re-alleged here.

25. From in or about August 2022 and continuing through in or about August 2023, in the Middle District of Tennessee and elsewhere, the defendant, **MATTHEW ISAAC KNOOT**, aiding and abetting DI and others known and unknown to the Grand Jury, knowingly caused and attempted to cause the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally caused damage without authorization to protected computers. The offense caused loss to one or more persons during a one-year period, and loss resulting from a related course of conduct affecting one or more other protected computers aggregating at least \$5,000 in value.

In violation of Title 18 United States Code, Sections 2, 1030(a)(5)(A), (c)(4)(B), and (c)(4)(A)(i)(I).

COUNT FIVE
(Aggravated Identity Theft)

26. The allegations in Paragraphs 1 through 25 of this Indictment are re-alleged here.

27. On or about the dates set forth below, in the Middle District of Tennessee and

elsewhere within the jurisdiction of the Court, the defendant, **MATTHEW ISAAC KNOOT**, aiding and abetting DI and others known and unknown to the Grand Jury, did knowingly transfer, possess, and use, without lawful authority, a means of identification of another person, U.S. Victim 1 (Andrew M.), as defined in Title 18, United States Code, Section 1028(d)(7)(A), during and in relation to violations of Title 18, United States Code, Sections 1030(a)(5)(A) and 1343, knowing that the means of identification belonged to another actual person:

Count	Victim	Approximate Dates	Means of Identification
4	U.S. Victim 1	July 11, 2022 August 1, 2022 August 8, 2022 August 9, 2022	First name, last name, date of birth, and social security number

In violation of Title 18, United States Code, Sections 1028A(a)(1) and 2).

COUNT SIX

(Conspiracy to Cause the Unlawful Employment of Aliens)

28. The allegations in Paragraphs 1 through 27 of this Indictment are re-alleged here.

29. From in or about July 2022 through at least August 2023, in the Middle District of Tennessee and elsewhere within the jurisdiction of the Court, the defendant, **MATTHEW ISAAC KNOOT**, together with others known and unknown to the Grand Jury, did knowingly conspire and agree to:

- a. hire, recruit, and refer for a fee, for employment in the United States, an alien, knowing the alien is an unauthorized alien with respect to such employment, in violation of Title 8, United States Code, Section 1324a(a)(1)(A) and 1324a(f)(1).

30. Specifically, between in or around July 2022 through at least August 2023, **KNOOT** and his Conspirators hired, recruited, and referred for a fee aliens, that is co-conspirator

YANG DI, an overseas IT worker, for employment in the United States, knowing that DI was not authorized for employment in the United States, with respect to such employment, as described in Count One.

In violation of Title 18, United States Code, Section 371.

FORFEITURE ALLEGATION

31. Upon conviction of any of the offenses alleged in Counts One through Five of this Indictment, the defendant, **MATTHEW ISAAC KNOOT**, shall forfeit to the United States any property, real or personal, which constitutes or is derived from proceeds traceable to these offenses, pursuant to Title 18, United States Code, Section 981(a)(1)(A) and (C), 1030(i), and Title 28, United States Code, Section 2461(c). The United States will also seek a forfeiture money judgment against the defendant for a sum of money equal to the value of any property, real or personal, which constitutes or is derived from proceeds traceable to these offenses.

32. Upon conviction of the offense alleged in Counts One through Four of this Indictment, the defendant shall forfeit to the United States any property constituting, or derived from, proceeds the defendant obtained directly or indirectly, as the result of this violation, pursuant to Title 18, United States Code, Section 982(a)(1) and (2) and 1030(i). The United States will also seek a forfeiture money judgment against the defendant for a sum of money equal to the value of any property constituting, or derived from, proceeds the defendant obtained directly or indirectly, as the result of these offenses.

33. If any of the property described above as being subject to forfeiture, as a result of any act or omission of the defendant:

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third party;
- c. has been placed beyond the jurisdiction of the Court;

- d. has been substantially diminished in value; or
- e. has been commingled with other property that cannot be divided without difficulty;

the defendant shall forfeit to the United States any other property of the defendant, up to the value of the property described above, pursuant to Title 21, United States Code, Section 853(p).


Pursuant to Title 18, United States Code, Sections 981(a)(1)(A) and (C); Title 18, United States Code, Sections 982(a)(1) and (2)(B); Title 18, United States Code, Section 1030(i); Title 28, United States Code, Section 2451(c); and Title 21, United States Code, Section 853(p)).

A TRUE BILL:


FOREPERSON

HENRY C. LEVENTIS
UNITED STATES ATTORNEY


JOSHUA KURTZMAN
ASSISTANT UNITED STATES ATTORNEY


GREGORY J. NICOSIA, JR.
TRIAL ATTORNEY